k-Resilient Identity-Based Encryption in the Standard Model [⋆]

Swee-Huay Heng[1] and Kaoru Kurosawa[2]

[1] Faculty of Information Science and Technology,
Multimedia University,
Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia.
shheng@mmu.edu.my

[2] Department of Computer and Information Sciences,
Ibaraki University,
4-12-1 Nakanarusawa, Hitachi, Ibaraki 316-8511, Japan
kurosawa@cis.ibaraki.ac.jp

Abstract. We present and analyze an adaptive chosen ciphertext secure (IND-CCA) identity-based encryption scheme (IBE) based on the well studied Decisional Diffie-Hellman (DDH) assumption. The scheme is provably secure in the *standard model* assuming the adversary can corrupt up to a maximum of k users adaptively. This is contrary to the Boneh-Franklin scheme which holds in the *random-oracle model.*

Key words: identity-based encryption, standard model

1 Introduction

The idea of identity-based encryption scheme (IBE) was formulated by Shamir [22] in 1984. Shamir's original motivation was to simplify certificate management in email systems. Some additional applications of IBE schemes include key escrow/recovery, revocation of public keys and delegation of decryption keys [5, 6].

An IBE scheme is an asymmetric system wherein the public key is effectively replaced by a user's publicly available identity information or any arbitrary string which derived from the user's identity. It enables any pair of users to communicate securely without exchanging public or private keys and without keeping any key directories. The service of a third party which we called Private Key Generator (PKG) is needed whose sole purpose is to generate private key for the user. The private key is computed using the PKG's master-key and the identity of the user. Key escrow is inherent in an IBE scheme since the PKG knows the private keys of all the users.

Since the presentation of the idea in 1984, several IBE schemes have emerged in the literature, based on various hard problems, for example [11, 24, 25, 19, 16, 8, 23]. Unfortunately, most of the proposed schemes are impractical.

[⋆] This is an extended version of a paper presented at CT-RSA 2004 [15].

A practical and functional IBE scheme was proposed by Boneh and Franklin in 2001 [5, 6]. Their scheme is adaptive chosen ciphertext secure (IND-CCA) in the random oracle model based on the Bilinear Diffie-Hellman (BDH) assumption, a natural analogue of the computational Diffie-Hellman problem. Specifically, the system is based on bilinear maps between groups realized through the Weil pairing or Tate pairing. The computational cost of the pairing is high compared to the computation of the power operation over finite fields.

However this scheme is still dissatisfactory due to two main issues: (1) its security was not proven under the standard model; (2) there is no evidence that BDH problem is indeed hard. Indeed, a security proof in the random oracle model is only a heuristic proof. These types of proofs have some limitations. In particular, they do not rule out the possibility of breaking the scheme without breaking the underlying intractability assumption. There exist digital signature schemes and public key encryption schemes which are secure in the random oracle model, but for which any implementation yields insecure schemes, as shown by Canetti et al. [7]. It is mentioned in [27] that BDH is reducible to most of the older believed-to-be-hard discrete logarithm problems and Diffie-Hellman (DH) problems, but there is no known reduction from any of those problems to BDH. As a result, we have no evidence that BDH problem is indeed hard.

In this paper, we somewhat manage to answer part of the open problem posed by Boneh and Franklin [5, 6], that is the possibility of building a chosen ciphertext secure IBE scheme under the standard computation model (rather than the random oracle model). We present and analyze an IND-CCA secure IBE scheme based on the DDH assumption. Our scheme is k-resilient, which means that the malicious adversary can corrupt up to a maximum of k users adaptively and thus possesses the k corresponding private keys. However, she cannot obtain any information pertinent to ciphertexts that are encrypted with public identities not belong to the corrupt users.

We adopt the technique of Cramer-Shoup [9, 10] in our construction. More precisely, we use a polynomial-based approach as in [17, 18, 12], but their ultimate goal is different from us in that their concern is more on traitor tracing and revocation. For completeness, we also provide an IND-CPA secure IBE scheme for the non-adaptive setting and the adaptive setting, respectively. The non-adaptive IND-CPA scheme is adapted from the El-Gamal scheme [14] and we incorporate the Pedersen commitments [20] in order to handle adaptive adversaries.

For the security proof, we adopt a simple variant of the chosen ciphertext security definition for IBE system in [5], which is slightly stronger than the standard definition for chosen ciphertext security [21]. First, the adversary is allowed to obtain from the PKG the private keys for at most k public identities of her choice adaptively. This models an adversary who obtains at most k private keys corresponding to some public identities of her choice and tries to attack some other public identity ID of her choice. Second, the adversary is challenged on an arbitrary public identity ID of her choice rather than a random public key.

Table 1. A comparison

	Model	Assumption	Number of malicious users
BF scheme	Random oracle	BDH	No limit
Proposed scheme	Standard	DDH	At most k

A comparison of Boneh-Franklin (BF) scheme and our proposed scheme is given in Table 1. This table shows a trade-off between (model, assumption) and the number of malicious users. BF scheme requires a stronger (model, assumption), but there is no limit on the number of malicious users. Our scheme requires a weaker (model, assumption), but the number of malicious users is limited to at most k. This limitation arises at the sacrifice of the use of random oracles and thus it seems to be unavoidable.

We argue, however, that the limit on the number of malicious users is not a serious problem in the real world. Indeed, it is not easy to corrupt a large number of users normally, meaning that the size of a malicious coalition cannot be unreasonably large. In another paper [4], Boneh and Franklin mentioned that it may suffice for k to be a fairly small integer, e.g. on the order of 20, but this is applicable to the traitor tracing scheme. Since our goal is different from theirs, we may use larger k if necessary, depending on the application, for example in some cases $k = 100$ may be sufficient.

Further, our scheme may be even practical in some circumstances. For instance, in a company or organization whereby the total number of users is small and higher security level is of paramount importance, our scheme is preferred to the BF scheme since our scheme is more reliable in that it is provably secure in the standard model under the well-known DDH assumption (as compared to the BF scheme which is proven secure in the random oracle model based on the much less analyzed BDH assumption). Specifically, our scheme can provide optimum security in the particular scenario wherein the total number of users n is less than or equal to k.

The efficiency of our scheme is linear in k and it is independent of the total number of users n. In other words, there exists trade-off between the efficiency of our scheme and the resilience k, hence the security level.

Related Work. Independently, Dodis et al. showed key-insulated encryption schemes [13], where their schemes coincide with our schemes. However, [13] did not present any formal definition nor security proof on ID-based encryption.

Remark. After our result has been published in [15], some other IBE schemes [2, 3, 1] have been proposed recently. In [2], Boneh and Boyen proposed two schemes which are provably secure in the standard model, in a slightly weaker security model, the so called *selective-ID* model, meaning that the adversary must commit ahead of time (non-adaptively) to the identity it intends to attack. The security of these two schemes are based on the intractability of two very specific and not well-studied problems respectively, namely, the decisional bilinear Diffie-Hellman

(DBDH) problem and the decisional bilinear Diffie-Hellman inversion (DBDHI) problem. In [3], the same authors proposed a fully secure IBE scheme in the standard model whose security is based on the DBDH assumption. However, the main shortcoming of the above scheme is that it is impractical, as mentioned by the authors themselves [3]. Notice that all the above mentioned schemes employ the property of pairings over elliptic curves. Another recent result is due to Au and Wei where they proposed an IBE scheme based on the composite degree residuosity (CDR) assumption [1]. However, this scheme is inefficient as it encrypts only one single bit at a time. Furthermore, its security relies on the random oracle heuristic. The most recent result is due to Waters [26] where he presented the first efficient IBE scheme that is fully secure in the standard model. The security of his scheme is based on the hardness of the DBDH problem. However, this scheme also employs the property of pairings over elliptic curves.

Organization. The rest of the paper is organized as follows. Some preliminaries such as basic facts, definitions and security models are given in Section 2. In Section 3, we present our proposed k-resilient IND-CPA schemes in the non-adaptive and adaptive settings. In Section 4, a k-resilient adaptive IND-CCA scheme is presented. Finally, some concluding remarks are made in Section 5.

2 Preliminaries

Lagrange Interpolation. Let q be a prime and $f(x)$ a polynomial of degree k in Z_q; let $j_0, \ldots, j_k$ be distinct elements in Z_q, and let $f_0 = f(j_0), \ldots, f_k = f(j_k)$. Using Lagrange Interpolation, we can express the polynomial as $f(x) \overset{\triangle}{=} \sum_{t=0}^{k}(f_t.\lambda_t(x))$, where $\lambda_t(x) \overset{\triangle}{=} \prod_{0 \le i \ne t \le k} \frac{j_i - x}{j_i - j_t}, t = 0, \ldots, k$, are the Lagrange coefficients.

DDH Assumption. The security of our schemes will rely on the Decisional Diffie-Hellman (DDH) assumption in a group G: namely, it is computationally hard to distinguish a quadruplet $R = \langle g_1, g_2, u_1, u_2 \rangle$ of four independent elements in G from a quadruplet $D = \langle g_1, g_2, u_1, u_2 \rangle$ satisfying $\log_{g_1} u_1 = \log_{g_2} u_2$.

BDH Assumption. We briefly review the BDH assumption which is used as the underlying assumption for Boneh-Franklin scheme. Let G_1 and G_2 be two groups of prime order q. Let $e : G_1 \times G_1 \rightarrow G_2$ be an admissible bilinear map and let P be a generator of G_1. The BDH assumption in (G_1, G_2) is such that given (P, aP, bP, cP) for some $a, b, c \in Z_q^*$, it is computationally hard to compute $e(P, P)^{abc} \in G_2$.

Collision-Resistant Hash Function. A family of hash functions is said to be collision resistance if given a randomly chosen hash function H from the family, it is infeasible for an adversary to find two distinct messages m and m' such that $H(m) = H(m')$.

IBE Scheme. An identity-based encryption scheme IBE is specified by four polynomially bounded algorithms: Setup, Extract, Encrypt, Decrypt where:

Setup. A probabilistic algorithm used by the PKG to set up all the parameters of the scheme. The Setup algorithm takes as input a security parameter 1^λ and a number k (i.e. the maximum number of users that can be corrupted) and generates the global system parameters params and master-key. The system parameters will be publicly known while the master-key will be known to the PKG only.

Extract. A probabilistic algorithm used by the PKG to extract a private key corresponding to a given public identity. The Extract algorithm receives as input the master-key and a public identity ID associated with the user; it returns the user's private key SK_{ID}.

Encrypt. A probabilistic algorithm used to encrypt a message m using a public identity ID. The Encrypt algorithm takes as input the system parameters params, a public identity ID and a message m and returns the ciphertext C.

Decrypt. A deterministic algorithm that takes as input the system parameters params, the private key SK_{ID} and the ciphertext C and returns the message m. We require that for all messages m, $\mathsf{Decrypt}(\mathsf{params}, SK_{\mathsf{ID}}, C) = m$ where $C = \mathsf{Encrypt}(\mathsf{params}, \mathsf{ID}, m)$.

Security. Chosen ciphertext security (IND-CCA) is the strongest notion of security for a public key encryption scheme. Hence, it is desirable to devise an IND-CCA secure IBE scheme. However, the definition of chosen ciphertext security in an identity-based system must be strengthened a bit for the following reason. When an adversary attacks a public identity ID, she might already possess the private keys of users $\mathsf{ID}_1, \mathsf{ID}_2, \ldots, \mathsf{ID}_k$ of her choice. We refer to these users as corrupt users. Hence, the definition of IND-CCA must allow the adversary to issue a maximum of k private key extraction queries adaptively. That is, the adversary is permitted to obtain the private keys associated with a maximum of k public identities of her choice adaptively (other than the public identity ID being attacked). Another difference is that the adversary is challenged on a public identity ID of her choice as opposed to a random public key. The two amendments apply to adaptive IND-CPA definition as well based on the same reasoning. We give the attack scenarios for IND-CPA and IND-CCA as follows:

IND-CPA. First, Setup is run and the adversary A is given the system parameters params. Then, A enters the private key extraction query stage, where she is given oracle access to the extraction oracle. This oracle receives as input the public identity ID_i and returns the corresponding private key SK_i. This oracle can be called adaptively for at most k times.

In the second stage, A can query the encryption oracle (also known as left-or-right oracle) on any pair of messages m_0, m_1 and an identity ID on which it wishes to be challenged. [3] Then, σ is chosen at random from $\{0, 1\}$ and the en-

[3] For the sake of generality, we could have allowed A to interleave the calls to the extraction oracle and the encryption oracle. However, this definition is equivalent to the one we present.

cryption oracle returns the challenge ciphertext $C^* = \mathsf{Encrypt}(\mathsf{params}, \mathsf{ID}, m_\sigma)$. Without loss of generality, we can assume that the encryption oracle is called exactly once. At the end of this stage, A outputs a bit σ^* which she thinks is equal to σ. We define the *advantage* of A as $\mathsf{Adv}^{\mathsf{IND-CPA}}_{\mathsf{IBE},A}(\lambda) := |\Pr[\sigma^* = \sigma] - \frac{1}{2}|$.

Remark. For the non-adaptive IND-CPA security, we must assume that the adversary has successfully corrupted the maximum of k users and thus obtained the k corresponding private keys before Setup takes place i.e. before the adversary learns the system parameters params. This is a weaker notion of security.

IND-CCA. The attack scenario is almost the same as that in the adaptive IND-CPA, except that now A has also access to the decryption oracle, which she can query on any pair $\langle \mathsf{ID}_i, C_i \rangle$ of her choice, where C_i is the chosen ciphertext. A can call this oracle at any point during the execution, both in the first and in the second stage, arbitrarily interleaved with her other oracle calls. To prevent the adversary from directly decrypting her challenge ciphertext C^*, the adversary is disallowed to query the decryption oracle on the pair $\langle \mathsf{ID}, C^* \rangle$ which is the output from the encryption oracle (i.e. $\langle \mathsf{ID}_i, C_i \rangle \neq \langle \mathsf{ID}, C^* \rangle$). As before, we define the advantage as $\mathsf{Adv}^{\mathsf{IND-CCA}}_{\mathsf{IBE},A}(\lambda) := |\Pr[\sigma^* = \sigma] - \frac{1}{2}|$.

Definition 1. *(k-resilience of an IBE Scheme)*
Let $\mu \in \{$IND-CPA,IND-CCA$\}$. We say that an IBE scheme is k-resilient against a μ-type attack if the advantage, $\mathsf{Adv}^{\mu}_{\mathsf{IBE},A}(\lambda)$, of any probabilistic polynomial-time (PPT) algorithm A is a negligible function of λ.

Before continuing, we state the following useful lemma which would be referred later [10].

Lemma 1. *Let U_1, U_2 and F be events defined on some probability space. Suppose that $(U_1 \wedge \neg F)$ and $(U_2 \wedge \neg F)$ are equivalent events, then $|\Pr[U_1] - \Pr[U_2]| \leq \Pr[F]$.*

3 k-Resilient IND-CPA Secure Schemes

In this section, we present two IBE schemes, a basic scheme which is k-resilient in the non-adaptive setting of an IND-CPA attack and an adaptive IND-CPA secure scheme. Subsequent schemes can be built on the previous one, in an incremental way, so that it is possible to obtain increasing security at the cost of slight efficiency loss.

3.1 Non-Adaptive IND-CPA Secure Scheme (Basic Scheme)

First we describe the basic scheme achieving semantically secure against chosen plaintext attack, assuming DDH problem is hard in the group G. This scheme is k-resilience in the non-adaptive setting.

Setup. Given a security parameter 1^λ and k, the algorithm works as follows. The first step is to define a multiplicative group G of prime order q of λ-bit long in which DDH assumption is believed to hold. For example, this is accomplished by selecting a random λ-bit long prime q such that $p = 2q + 1$ is also prime, and a random element g of order q modulo p. The group G is then set to be the subgroup of Z_p^* generated by g, i.e. $G = \{g^i \bmod p : i \in Z_q\} \subset Z_p^*$. Note that the exponent of g works in $GF(q)$. Then, a random k-degree polynomial $f(x) \overset{\triangle}{=} \sum_{t=0}^{k} d_t x^t$ is chosen over Z_q. Finally, the algorithm publicizes the system parameters $\mathsf{params} = \langle g, g^{d_0}, \ldots, g^{d_k} \rangle$. The $\mathsf{master\text{-}key}$ is $f(x)$ which is known to the PKG only.

Extract. For a given public identity $\mathsf{ID} \in Z_q$, the algorithm computes $f_{\mathsf{ID}} = f(\mathsf{ID})$ from the PKG's $\mathsf{master\text{-}key}$.

Encrypt. To encrypt a message $m \in G$ under the public identity ID, the algorithm computes $s = (\prod_{t=0}^{k} g^{d_t \mathsf{ID}^t})^r$ $(= (g^{f_{\mathsf{ID}}})^r)$ where $r \in Z_q$ is a random value. Next, it sets the ciphertext as $C = \langle g^r, m \cdot s \rangle$.

Decrypt. Let $C = \langle c_1, c_2 \rangle$ be a ciphertext encrypted using the public identity ID. To decrypt C using the private key f_{ID}, the algorithm computes $m = c_2 / c_1^{f_{\mathsf{ID}}}$.

Recall that $D = (g_1, g_2, g_1^r, g_2^r)$ and $R = (g_1, g_2, g_1^r, g_2^{r'})$ where g_1, g_2 are generators and r, r' such that $r \neq r'$ are randomly chosen over Z_q. In the proof of the following theorem, by Lagrange interpolation, $f(x)$ can be expressed as $f(x) \overset{\triangle}{=} \sum_{t=0}^{k} (f_t . \lambda_t(x))$, where $f_t = f(\mathsf{ID}_t)$ and $\lambda_t(x) = \prod_{0 \le i \neq t \le k} \frac{\mathsf{ID}_i - x}{\mathsf{ID}_i - \mathsf{ID}_t}, t = 0, \ldots, k$.

Theorem 1. *The above basic scheme is k-resilient against the non-adaptive chosen plaintext attack (IND-CPA) under the DDH assumption.*

Proof. Suppose that the adversary A attacks the above IBE scheme successfully in terms of non-adaptive IND-CPA security with non-negligible advantage, we show that there is a PPT algorithm A_1 that distinguishes D from R with a non-negligible advantage.

Assume that A successfully corrupts up to k users of its choice and hence obtains the k corresponding private keys. Given the k private keys and the system parameters $\mathsf{params} = \langle g, g^{d_0}, \ldots, g^{d_k} \rangle$, A finds two messages m_0 and m_1 in G and outputs an identity ID on which it wishes to be challenged such that it can distinguish them by observing the ciphertext.

Let (g_1, g_2, u_1, u_2) be the input of algorithm A_1. Algorithm A_1 shall decide whether (g_1, g_2, u_1, u_2) is from D or R by working as follows:

1. For notational convenience, we deserve the indices $1, \ldots, k$ for the corrupt users. Choose k private keys $f_1, \ldots, f_k$ at random corresponding to the k corrupt users' public identities $\mathsf{ID}_1, \ldots, \mathsf{ID}_k$. Let $g = g_1, g^{d_0} = g_2$. Compute $g^{d_1}, \ldots, g^{d_k}$ as follows. Notice that, $f_1, \ldots, f_k$ can be written in the matrix

form as follows:

$$\begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_k \end{pmatrix} = \begin{pmatrix} d_0 \\ d_0 \\ \vdots \\ d_0 \end{pmatrix} + \underbrace{\begin{pmatrix} \mathsf{ID}_1 & \mathsf{ID}_1^2 & \cdots & \mathsf{ID}_1^k \\ \mathsf{ID}_2 & \mathsf{ID}_2^2 & \cdots & \mathsf{ID}_2^k \\ \vdots & \vdots & \ddots & \vdots \\ \mathsf{ID}_k & \mathsf{ID}_k^2 & \cdots & \mathsf{ID}_k^k \end{pmatrix}}_{M} \cdot \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_k \end{pmatrix}$$

where matrix M is a Vandermonde matrix. It is clear that M is non-singular since $\mathsf{ID}_1, \ldots, \mathsf{ID}_k$ are all distinct. Therefore, we have

$$(d_1, \ldots, d_k)^T = M^{-1}(f_1 - d_0, \ldots, f_k - d_0)^T.$$

Let $(b_{t1}, \ldots, b_{tk})$ be the t-th row of M^{-1}. Then

$$\begin{aligned} d_t &= b_{t1}(f_1 - d_0) + \cdots + b_{tk}(f_k - d_0) \\ &= b_{t1}f_1 + \cdots + b_{tk}f_k - (b_{t1} + \cdots + b_{tk})d_0. \end{aligned}$$

Hence $g^{d_t} = g_1^{b_{t1}f_1 + \cdots + b_{tk}f_k} / g_2^{b_{t1} + \cdots + b_{tk}}, \quad t = 1, 2, \ldots, k.$

Let $f'(x) = \sum_{t=1}^{k} f_t \lambda_t(x)$ and $f(x) = f'(x) + d_0\lambda_0(x)$ where $\lambda_t(x)$ is computed from $\mathsf{ID}_0 = 0$ and $\mathsf{ID}_1, \ldots, \mathsf{ID}_k$. Note that we do not know $d_0 = f_0$.

2. Feed the private keys $f_1, \ldots, f_k$ and the system parameters $\mathsf{params} = \langle g_1, g_2, g^{d_1}, \ldots, g^{d_k} \rangle$ to A. A returns $m_0, m_1 \in G$ and an identity ID such that $\mathsf{ID} \notin \{\mathsf{ID}_1, \ldots, \mathsf{ID}_k\}$.
3. Randomly select $\sigma \in \{0, 1\}$ and encrypt m_σ as $C^* = \langle u_1, m_\sigma \cdot s \rangle$ where $s = u_1^{f'(\mathsf{ID})} \cdot u_2^{\lambda_0(\mathsf{ID})}$.
4. Feed C^* to A and get a return σ^*. The algorithm outputs 1 if and only if $\sigma = \sigma^*$.

If (g_1, g_2, u_1, u_2) is from D, $g = g_1$, $g_2 = g^{d_0}$, $u_1 = g^r$, $u_2 = g_2^r = g^{rd_0}$ and $u_1{}^{f'(\mathsf{ID})} \cdot u_2^{\lambda_0(\mathsf{ID})} = g^{r\sum_{t=1}^{k} f_t\lambda_t(\mathsf{ID})} g^{rd_0\lambda_0(\mathsf{ID})} = g^{r\sum_{t=0}^{k} f_t\lambda_t(\mathsf{ID})} = g^{rf_{\mathsf{ID}}} = s$. Thus C^* is the encryption of m_σ and $\Pr[A_1(g_1, g_2, u_1, u_2) = 1] = \Pr[A(C^*) = \sigma] = \frac{1}{2} + \epsilon_1$, for some non-negligible advantage ϵ_1. Otherwise, since $u_1 = g_1^r, u_2 = g_2^{r'}$, the distribution of C^* is the same for both $\sigma = 0$ and $\sigma = 1$. Thus $\Pr[A_1(g_1, g_2, u_1, u_2) = 1] = \Pr[A(C^*) = \sigma] = \frac{1}{2}$. Therefore, A_1 distinguishes D from R with a non-negligible advantage ϵ_1. □

3.2 Adaptive IND-CPA Secure Scheme

In this section, we present an adaptive IND-CPA secure IBE scheme with the condition that the adversary can corrupt up to a maximum of k users adaptively.

For this scheme and the scheme in Section 4, our proofs follow the structural approach advocated in [10] by defining a sequence of attack games $\mathbf{G}_0, \mathbf{G}_1, \ldots, \mathbf{G}_l$, all operating under the same underlying probability space. Starting from $\mathbf{G}_0$, we make slight modifications to the behavior of the oracles, thus changing the way the adversary's view is computed, while maintaining the view's distributions indistinguishable among the games. We emphasize that the different games do not change the encryption algorithm (and decryption algorithm) but the encryption oracle (and decryption oracle), i.e. the method in which the challenge ciphertext is generated (and the ciphertext is decrypted) only. The actual encryption algorithm (and decryption algorithm) that the scheme (and hence the attacker) uses remains the same.

For any $1 \leq i \leq l$, let T_i be the event that $\sigma = \sigma^*$ in game $\mathbf{G}_i$. Our strategy is to show that for $1 \leq i \leq l$, the quantity $|\Pr[T_i] - \Pr[T_{i-1}]|$ is negligible. Also, it will be evident from the definition of game $\mathbf{G}_l$ that $\Pr[T_l] = \frac{1}{2}$, which will imply that $|\Pr[T_0] - \frac{1}{2}|$ is negligible.

Setup. It is almost the same as in the basic scheme except that in this scheme we use two generators. This is accomplished selecting a random element g_1 of order q modulo p. The group G is set to be the subgroup of Z_p^* generated by g_1, i.e. $G = \{g_1^i \bmod p : i \in Z_q\} \subset Z_p^*$. A random $w \leftarrow_{\mathrm{R}} Z_q$ is then chosen and used to compute $g_2 = g_1^w$. Then, two random k-degree polynomials

$$p_1(x) \triangleq \sum_{t=0}^{k} d_t x^t \quad \text{and} \quad p_2(x) \triangleq \sum_{t=0}^{k} d'_t x^t$$

are chosen over Z_q. Next, the algorithm computes $D_0 = g_1^{d_0} g_2^{d'_0}, \ldots, D_k = g_1^{d_k} g_2^{d'_k}$. Finally, it publicizes the system parameters as $\mathsf{params} = \langle g_1, g_2, D_0, \ldots, D_k \rangle$. The $\mathsf{master\text{-}key}$ is $\langle p_1, p_2 \rangle$ which is known to the PKG only.

Extract. For a given public identity $\mathsf{ID} \in Z_q$, the algorithm computes $p_{1,\mathsf{ID}} = p_1(\mathsf{ID})$ and $p_{2,\mathsf{ID}} = p_2(\mathsf{ID})$ [4] and returns $d = \langle p_{1,\mathsf{ID}}, p_{2,\mathsf{ID}} \rangle$.

Encrypt. To encrypt a message $m \in G$ under the public identity ID, the working steps of the encryption algorithm are given in Fig. 1.

Decrypt. To decrypt C using the private key $d = \langle p_{1,\mathsf{ID}}, p_{2,\mathsf{ID}} \rangle$, the decryption algorithm is depicted in Fig. 1.

Encryption algorithm	Decryption algorithm
$E1.\ r_1 \leftarrow_{\mathrm{R}} Z_q$ $E2.\ u_1 \leftarrow g_1^{r_1}$ $E3.\ u_2 \leftarrow g_2^{r_1}$ $E4.\ s \leftarrow (\prod_{t=0}^{k} D_t^{\mathsf{ID}^t})^{r_1}$ $E5.\ c \leftarrow m \cdot s$ $E6.\ C \leftarrow \langle u_1, u_2, c \rangle$	$D1.\ s \leftarrow u_1^{p_{1,\mathsf{ID}}} \cdot u_2^{p_{2,\mathsf{ID}}}$ $D2.\ m \leftarrow c \cdot s^{-1}$

Fig. 1. Encryption and decryption algorithms for the IND-CPA secure scheme

[4] For conciseness, we will follow this notation hereafter.

Theorem 2. *The above IBE scheme is k-resilient against adaptive chosen plaintext attack (IND-CPA) under the DDH assumption.*

Proof. We shall define a sequence of "indistinguishable" modified attack games $\mathbf{G}_0$, $\mathbf{G}_1$, $\mathbf{G}_2$ and $\mathbf{G}_3$ where $\mathbf{G}_0$ is the original game and the last game clearly gives no advantage to the adversary.
Game $\mathbf{G}_0$. In game $\mathbf{G}_0$, the adversary A receives the system parameters $\mathsf{params} = \langle g_1, g_2, D_0, \ldots, D_k\rangle$ and adaptively queries the extraction oracle for a maximum of k public identities of its choice. Then, it outputs a challenge identity ID and queries the encryption oracle on (m_0, m_1). A receives the ciphertext C^* as the answer. At this point, A outputs its guess $\sigma^* \in \{0,1\}$. Let T_0 be the event that $\sigma = \sigma^*$ in game $\mathbf{G}_0$.
Game $\mathbf{G}_1$. Game $\mathbf{G}_1$ is identical to game $\mathbf{G}_0$, except for a small modification to the encryption oracle. In game $\mathbf{G}_1$, step $E4$ of the encryption algorithm in Fig. 1 is replaced with the following step:

$$E4'. \quad s \leftarrow u_1^{p_{1,\mathsf{ID}}} \cdot u_2^{p_{2,\mathsf{ID}}}$$

It is clear that step $E4'$ computes the same value as step $E4$. The point of this change is to make explicit any functional dependency of the above quantity on u_1 and u_2. Let T_1 be the event that $\sigma = \sigma^*$ in game $\mathbf{G}_1$. Clearly, it holds that $\Pr[T_0] = \Pr[T_1]$.
Game $\mathbf{G}_2$. To turn game $\mathbf{G}_1$ into game $\mathbf{G}_2$, we make another change to the encryption oracle. We replace $E1$ and $E3$ with the following:

$$E1'.\ r_1 \leftarrow_{\mathrm{R}} Z_q, \quad r_2 \leftarrow_{\mathrm{R}} Z_q \backslash \{r_1\}$$
$$E3'.\ u_2 \leftarrow g_2^{r_2}$$

Let T_2 be the event that $\sigma = \sigma^*$ in game $\mathbf{G}_2$. Notice that while in game $\mathbf{G}_1$ the values u_1 and u_2 are obtained using the same value r_1, in game $\mathbf{G}_2$ they are independent subject to $r_1 \neq r_2$. Therefore, using a standard reduction argument, any non-negligible difference in behaviour between $\mathbf{G}_1$ and $\mathbf{G}_2$ can be used to construct a PPT algorithm A_1 that is able to distinguish Diffie-Hellman tuples from totally random tuples with non-negligible advantage. Hence $|\Pr[T_2] - \Pr[T_1]| \leq \epsilon_1$ for some negligible ϵ_1.
Game $\mathbf{G}_3$. In this game, we again modify the encryption oracle as follows:

$$E5'.\ e \leftarrow_{\mathrm{R}} Z_q, \quad c \leftarrow g_1^e$$

Let T_3 be the event that $\sigma = \sigma^*$ in game $\mathbf{G}_3$. Due to this last change, the challenge no longer contains σ, nor does any other information in the adversary's view. Therefore, we have that $\Pr[T_3] = \frac{1}{2}$. Moreover, we can prove that the adversary has the same chances to guess σ in both game $\mathbf{G}_2$ and $\mathbf{G}_3$, i.e. $\Pr[T_3] = \Pr[T_2]$. (see Appendix, Lemma 3).

Finally, combining all the intermediate results, we can conclude that adversary A's advantage is negligible. More precisely, $\mathsf{Adv}^{\mathsf{IND-CPA}}_{\mathsf{IBE},A}(\lambda) \leq \epsilon_1$. □

4 *k*-Resilient IND-CCA Secure Scheme

We present an identity-based encryption scheme achieving adaptive chosen ciphertext security in this section. This scheme makes use of a hash function chosen randomly from a family of collision-resistant hash functions. Again, this adaptive IND-CCA IBE scheme is secure against the adversary which can corrupt a maximum of k users adaptively. We give the description of the scheme as follows:

Setup. As in the previous scheme, the first task is to select a random multiplicative group $G \subset Z_p^*$ of prime order q and two generators $g_1, g_2 \in G$. Then, six random k-degree polynomials are chosen over Z_q. That is,

$$f_1(x) \triangleq \sum_{t=0}^{k} a_t x^t, \qquad f_2(x) \triangleq \sum_{t=0}^{k} a'_t x^t,$$

$$h_1(x) \triangleq \sum_{t=0}^{k} b_t x^t, \qquad h_2(x) \triangleq \sum_{t=0}^{k} b'_t x^t,$$

$$p_1(x) \triangleq \sum_{t=0}^{k} d_t x^t, \qquad p_2(x) \triangleq \sum_{t=0}^{k} d'_t x^t.$$

Next, the algorithm computes $A_t = g_1^{a_t} g_2^{a'_t}, B_t = g_1^{b_t} g_2^{b'_t}$ and $D_t = g_1^{d_t} g_2^{d'_t}$, for $t = 0, \ldots, k$ and chooses at random a hash function H from a family of collision-resistant hash functions. Finally, it publicizes the system parameters $\mathsf{params} = \langle g_1, g_2, A_0, \ldots, A_k, B_0, \ldots, B_k, D_0, \ldots, D_k, H\rangle$. The $\mathsf{master\text{-}key}$ is $\langle f_1, f_2, h_1, h_2, p_1, p_2\rangle$ which is known to the PKG only.

Extract. For a given public identity $\mathsf{ID} \in Z_q$, the algorithm returns $d = \langle f_{1,\mathsf{ID}}, f_{2,\mathsf{ID}}, h_{1,\mathsf{ID}}, h_{2,\mathsf{ID}}, p_{1,\mathsf{ID}}, p_{2,\mathsf{ID}}\rangle$.

Encrypt. To encrypt a message $m \in G$ under the public identity ID, the encryption algorithm works as depicted in Fig. 2.

Decrypt. To decrypt C using the private key $d = \langle f_{1,\mathsf{ID}}, f_{2,\mathsf{ID}}, h_{1,\mathsf{ID}} h_{2,\mathsf{ID}}, p_{1,\mathsf{ID}}, p_{2,\mathsf{ID}}\rangle$, the decryption algorithm is given in Fig. 2.

Theorem 3. *The above IBE scheme is k-resilient against adaptive chosen ciphertext attack (IND-CCA) suppose the DDH assumption holds for G and H is chosen from a family of collision-resistant hash functions.*

Proof. For convenience, we shall defer the proofs of all the lemmas to the end of the theorem. As in the proof of Theorem 2, we shall define a sequence of modified games $\mathbf{G}_i$, for $0 \leq i \leq 5$. Let T_i be the event that $\sigma = \sigma^*$ in game $\mathbf{G}_i$.

Game $\mathbf{G}_0$. In game $\mathbf{G}_0$, the adversary A receives the system parameters $\mathsf{params} = \langle g_1, g_2, A_0, \ldots, A_k, B_0, \ldots, B_k, D_0, \ldots, D_k, H\rangle$ and adaptively interleaves queries to the extraction oracle and the decryption oracle. For private key extraction query, A inputs the public identity ID_i of its choice while for the

Encryption algorithm	Decryption algorithm
$E1.\ r_1 \leftarrow_{\mathrm{R}} Z_q$	$D1.\ \alpha \leftarrow H(u_1, u_2, c)$
$E2.\ u_1 \leftarrow g_1^{r_1}$	$D2.$ Test if $v \leftarrow u_1^{f_{1,\mathsf{ID}}+h_{1,\mathsf{ID}}\alpha} \cdot u_2^{f_{2,\mathsf{ID}}+h_{2,\mathsf{ID}}\alpha}$; reject and halt if this is not the case
$E3.\ u_2 \leftarrow g_2^{r_1}$	
$E4.\ s \leftarrow (\prod_{t=0}^{k} D_t^{\mathsf{ID}^t})^{r_1}$	$D3.\ s \leftarrow u_1^{p_{1,\mathsf{ID}}} \cdot u_2^{p_{2,\mathsf{ID}}}$
$E5.\ c \leftarrow m \cdot s$	$D4.\ m \leftarrow c \cdot s^{-1}$
$E6.\ \alpha \leftarrow H(u_1, u_2, c)$	
$E7.\ v \leftarrow (\prod_{t=0}^{k} A_t^{\mathsf{ID}^t})^{r_1} \cdot (\prod_{t=0}^{k} B_t^{\mathsf{ID}^t})^{r_1\alpha}$	
$E8.\ C \leftarrow \langle u_1, u_2, c, v\rangle$	

Fig. 2. Encryption and decryption algorithms for the IND-CCA secure scheme

decryption query, A provides the oracle with the public identity and ciphertext pair $\langle \mathsf{ID}_i, C_i\rangle$ of its choice. A can query the extraction oracle for a maximum of k times adaptively. Then, A outputs a challenge identity ID and queries the encryption oracle on (m_0, m_1). It receives the ciphertext C^* as the answer. Next, A can again query the decryption oracle, restricted only in that $\langle \mathsf{ID}_i, C_i\rangle \neq \langle \mathsf{ID}, C^*\rangle$. Finally, A outputs its guess $\sigma^* \in \{0, 1\}$.

Game $\mathbf{G}_1$. Game $\mathbf{G}_1$ is identical to game $\mathbf{G}_0$, except for a small modification to the encryption oracle. In game $\mathbf{G}_1$, step $E4$ of the encryption algorithm in Fig. 2 is replaced with step $E4'$ and step $E7$ of the encryption algorithm in Fig. 2 is replaced with step $E7'$ as follows:

$$E4'.\ s \leftarrow u_1^{p_{1,\mathsf{ID}}} \cdot u_2^{p_{2,\mathsf{ID}}}$$
$$E7'.\ v \leftarrow u_1^{f_{1,\mathsf{ID}}+h_{1,\mathsf{ID}}\alpha} \cdot u_2^{f_{2,\mathsf{ID}}+h_{2,\mathsf{ID}}\alpha}$$

It is clear that steps $E4'$ and $E7'$ compute the same values as steps $E4$ and $E7$ respectively. The point of these changes is just to make explicit any functional dependency of the above quantities on u_1 and u_2. Clearly, it holds that $\Pr[T_0] = \Pr[T_1]$.

Game $\mathbf{G}_2$. To turn game $\mathbf{G}_1$ into game $\mathbf{G}_2$, we make another change to the encryption oracle. We replace $E1$ and $E3$ with the following:

$$E1'.\ r_1 \leftarrow_{\mathrm{R}} Z_q, \quad r_2 \leftarrow_{\mathrm{R}} Z_q \backslash \{r_1\}$$
$$E3'.\ u_2 \leftarrow g_2^{r_2}$$

Notice that while in game $\mathbf{G}_1$ the values u_1 and u_2 are obtained using the same value r_1, in game $\mathbf{G}_2$ they are independent subject to $r_1 \neq r_2$. Therefore, using a standard reduction argument, any non-negligible difference in behaviour between $\mathbf{G}_1$ and $\mathbf{G}_2$ can be used to construct a PPT algorithm A_1 that is able to distinguish Diffie-Hellman tuples from totally random tuples with non-negligible advantage. Hence $|\Pr[T_2] - \Pr[T_1]| \leq \epsilon_1$ for some negligible ϵ_1.

Game $\mathbf{G}_3$. To define game $\mathbf{G}_3$, we slightly modify the decryption oracle, replacing steps $D2$ and $D3$ with:

$D2'$. Test if $u_2 = u_1^w$ and
$v = u_1^{(f_{1,\mathsf{ID}}+h_{1,\mathsf{ID}}\alpha)+(f_{2,\mathsf{ID}}+h_{2,\mathsf{ID}}\alpha)w}$;
reject and halt if this is not the case
$D3'$. $s \leftarrow u_1^{p_{1,\mathsf{ID}}+wp_{2,\mathsf{ID}}}$

Let R_3 be the event that, some decryption query that would have passed the test in step $D2$ used in game $\mathbf{G}_2$ fails the test in step $D2'$ in game $\mathbf{G}_3$. Obviously, $\mathbf{G}_2$ and $\mathbf{G}_3$ are identical until event R_3 occurs. In particular, the events $(T_2 \ \wedge \neg R_3)$ and $(T_3 \ \wedge \neg R_3)$ are identical. By Lemma 1, we have $|\Pr[T_3] - \Pr[T_2]| \leq \Pr[R_3]$.

We introduce two more games, $\mathbf{G}_4$ and $\mathbf{G}_5$ in order to bound $\Pr[R_3]$.

Game $\mathbf{G}_4$. In this game, we again modify the encryption oracle as follows:

$$E5'.\ e \leftarrow_{\mathrm{R}} Z_q, \quad c \leftarrow g_1^e$$

Due to this change, the challenge no longer contains σ, nor does any other information in the adversary's view. Therefore, we have that $\Pr[T_4] = \frac{1}{2}$.

Let R_4 be the event that some decryption query that would have passed the test in step $D2$ used in game $\mathbf{G}_2$ fails the test in step $D2'$ in game $\mathbf{G}_4$. In Lemma 4 in the Appendix, we show that those events happen with the same probability as the corresponding events of game $\mathbf{G}_3$. More precisely, we prove that $\Pr[T_4] = \Pr[T_3]$ and $\Pr[R_4] = \Pr[R_3]$.

Game $\mathbf{G}_5$. This game is the same as game $\mathbf{G}_4$, except for the following modification. We modify the decryption oracle so that it applies the following *special rejection rule*, whose goal is to prevent the adversary from submitting illegal ciphertexts to the decryption oracle after it has received the challenge C^*.

Special rejection rule: After A receives its challenge $C^* = \langle u_1^*, u_2^*, c^*, v^* \rangle$, the decryption oracle rejects any query $\langle \mathsf{ID}_i, C_i \rangle$, with $C_i = \langle u_1, u_2, c, v \rangle$ such that $\langle \mathsf{ID}_i, u_1, u_2, c \rangle \neq \langle \mathsf{ID}, u_1^*, u_2^*, c^* \rangle$ but $\alpha = \alpha^*$. It does so before executing step $D2'$.

Let C_5 be the event that the adversary submits a decryption query that is rejected using the *special rejection rule*. Let R_5 be the event that A submits some decryption query that would have passed the test in step $D2$ used in game $\mathbf{G}_2$, but fails the test in step $D2'$ used in game $\mathbf{G}_5$. Clearly, $\mathbf{G}_4$ and $\mathbf{G}_5$ are identical until event C_5 occurs. In particular, the events $(R_4 \ \wedge \neg C_5)$ and $(R_5 \ \wedge \neg C_5)$ are identical. By Lemma 1, we have $|\Pr[R_5] - \Pr[R_4]| \leq \Pr[C_5]$.

We need to show that events C_5 and R_5 occur with negligible probability. The argument to bound event C_5 is based on the collision-resistant assumption. Using a standard reduction argument, we can construct a PPT algorithm A_2 that breaks the collision-resistant assumption with non-negligible advantage. Hence we have $\Pr[C_5] \leq \epsilon_2$ for some negligible ϵ_2. Subsequently, we show that event R_5 occurs with negligible probability purely based on some information-theoretic considerations. That is, $\Pr[R_5] \leq Q_A(\lambda)/q$, where $Q_A(\lambda)$ is an upper bound on the number of decryption queries made by the adversary. The detailed proof is given in Lemma 5 in the Appendix.

Finally, combining all the intermediate results, we can conclude that adversary A's advantage is negligible; more precisely: $\mathsf{Adv}_{\mathsf{IBE},A}^{\mathsf{IND-CCA}}(\lambda) \leq \epsilon_1 + \epsilon_2 + Q_A(\lambda)/q$. □

5 Conclusion

We proposed an adaptive IND-CCA secure IBE scheme based on the DDH assumption. The scheme is provably secure in the standard model assuming the adversary can corrupt up to a maximum of k users adaptively. We also presented a non-adaptive IND-CPA secure IBE scheme and an adaptive IND-CPA secure IBE scheme based on the same assumption. Proofs of security for all the proposed schemes are given in detail.

References

1. M. H. Au and Victor K. Wei, "ID-Based cryptography from composite degree residuosity," *IACR Cryptology ePrint Archive*, Report 2004/164, Available from `http://eprint.iacr.org/2004/164/`.
2. D. Boneh and X. Boyen, "Efficient selective-ID secure identity-based encryption without random oracles," *Advances in Cryptology — EUROCRYPT '04*, LNCS 3027, pp. 223–238, Springer-Verlag, 2004.
3. D. Boneh and X. Boyen, "Secure identity based encryption without random oracles," *Advances in Cryptology–CRYPTO '04*, LNCS 3152, pp.443–459, Springer-Verlag, 2004.
4. D. Boneh and M. Franklin, "An efficient public key traitor tracing scheme," *Advances in Cryptology — CRYPTO '99*, LNCS 1666, pp. 338–353, Springer-Verlag, 1999.
5. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *Advances in Cryptology — CRYPTO '01*, LNCS 2139, pp. 213–229, Springer-Verlag, 2001.
6. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *Siam Journal of Computing*, Vol. 32, pp. 586–615, 2003. Updated version of [5].
7. R. Canetti, O. Goldreich and S. Halevi, "The random oracle model, revisited," *30th Annual ACM Symposium on Theory of Computing — STOC '98*, pp. 209–218, 1998.
8. C. Cocks, "An identity based encryption scheme based on quadratic residues," *Cryptography and Coding*, LNCS 2260, pp. 360–363, Springer-Verlag, 2001.
9. R. Cramer and V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," *Advances in Cryptology — CRYPTO '98*, LNCS 1462, pp. 13–25, Springer-Verlag, 1998.
10. R. Cramer and V. Shoup, "Design and analysis of practical public-key encryption scheme secure against adaptive chosen ciphertext attack," *SIAM Journal of Computing*, vol. 33, no. 1, pp. 167–226, 2003.
11. Y. Desmedt and J. Quisquater, "Public-key systems based on the difficulty of tampering," *Advances in Cryptology — CRYPTO '86*, LNCS 0263, pp. 111–117, Springer-Verlag, 1986.
12. Y. Dodis and N. Fazio, "Public key trace and revoke scheme secure against adaptive chosen ciphertext attack," *Public Key Cryptography — PKC '03*, LNCS 2567, pp. 100–115, Springer-Verlag, 2003. Full version is available at `http://eprint.iacr.org/`.
13. Y. Dodis, J. Katz, S. Xu and M. Yung, "Key-insulated public key cryptosystems," *Advances in Cryptology — EUROCRYPT '02*, LNCS 2332, pp. 65–82, Springer-Verlag, 2002.

14. T. El Gamal, "A public-key cryptosystem and a signature scheme based on the discrete logarithm," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.
15. S.-H. Heng and K. Kurosawa, "k-Resilient identity-based encryption in the standard model," *Topics in Cryptology — CT-RSA '04*, LNCS 2964, pp. 67–80, Springer-Verlag, 2004.
16. D. Hühnlein, M. J. Jacobson and D. Weber, "Towards practical non-interactive public key cryptosystems using non-maximal imaginary quadratic orders," *Selected Areas in Cryptography — SAC '00*, LNCS 2012, pp. 275–287, Springer-Verlag, 2001.
17. K. Kurosawa and Y. Desmedt, "Optimum traitor tracing and asymmetric schemes," *Advances in Cryptology — EUROCRYPT '98*, LNCS 1403, pp. 145–157, Springer-Verlag, 1998.
18. K. Kurosawa and T. Yoshida, "Linear code implies public-key traitor tracing," *Public Key Cryptography — PKC '02*, LNCS 2274, pp. 172–187, Springer-Verlag, 2002.
19. U. Maurer and Y. Yacobi, "Non-interactive public-key cryptography," *Advances in Cryptology — EUROCRYPT '91*, LNCS 0547, pp. 498–507, Springer-Verlag, 1991.
20. T. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," *Advances in Cryptology — CRYPTO '91*, LNCS 0576, pp. 129–140, Springer-Verlag, 1992.
21. C. Rackoff and D. Simon, "Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack," *Advances in Cryptology — CRYPTO '91*, LNCS 0576, pp. 433–444, Springer-Verlag, 1992.
22. A. Shamir, "Identity-based cryptosystems and signature schemes," *Advances in Cryptology — CRYPTO '84*, LNCS 0196, pp. 47–53, Springer-Verlag, 1985.
23. R. Sakai, K. Ohgishi and M. Kasahara, "Cryptosystems based on pairing over elliptic curve," *Symposium on Cryptography and Information Security — SCIS '01*, pp. 369–372, 2001 (In Japanese).
24. H. Tanaka, "A realization scheme for the identity-based cryptosystem," *Advances in Cryptology — CRYPTO '87*, LNCS 0293, pp. 341–349, Springer-Verlag, 1987.
25. S. Tsuji and T. Itoh, "An ID-based cryptosystem based on the discrete logarithm problem," *IEEE Journal on Selected Areas in Communication*, vol. 7, no. 4, pp. 467–473, 1989.
26. R. Waters, "Efficient identity-based ecryption without random oracles," To appear in *Advances in Cryptology — EUROCRYPT '05*, 2005. Available from `http://eprint.iacr.org/2004/180/`.
27. Y. Yacobi, "A note on the bilinear Diffie-Hellman assumption," *IACR Cryptology ePrint Archive, Report 2002/113.* Available from `http://eprint.iacr.org/2002/113/`.

APPENDIX

The proofs of the following lemmas are based on the same techniques used in [10]; the main tool is the following technical lemma.

Lemma 2. *Let m, n be integers with $1 \leq m \leq n$, and let K be a finite field. Consider a probability space with random variables $\boldsymbol{\alpha} \in K^{n \times 1}, \boldsymbol{\beta} = (\beta_1, \ldots, \beta_m)^T \in$*

$K^{m\times 1}, \boldsymbol{\gamma} \in K^{m\times 1}$, and $M \in K^{m\times n}$, such that $\boldsymbol{\alpha}$ is uniformly distributed over $K^n, \boldsymbol{\beta} = M\boldsymbol{\alpha} + \boldsymbol{\gamma}$, and for $1 \le i \le m$, the first ith rows of M and $\boldsymbol{\gamma}$ are determined by $\beta_1, \ldots, \beta_{i-1}$. Then, conditioning on any fixed values of $\beta_1, \ldots, \beta_{m-1}$ such that the resulting matrix M has rank m, the value of β_m is uniformly distributed over K in the resulting conditional probability space.

In what follows, we will denote with $Coins$ the coin tosses of an adversary A. For any t, we define

$$f_{\mathsf{ID}_t} := f_{1,\mathsf{ID}_t} + wf_{2,\mathsf{ID}_t}, h_{\mathsf{ID}_t} := h_{1,\mathsf{ID}_t} + wh_{2,\mathsf{ID}_t}, p_{\mathsf{ID}_t} := p_{1,\mathsf{ID}_t} + wp_{2,\mathsf{ID}_t}.$$

Proof of the Lemma stated in Theorem 2

Lemma 3. $\Pr[T_3] = \Pr[T_2]$.

Proof. Consider the quantities

$$V := (Coins, w, \sigma, r_1^*, r_2^*)$$

and the value p_{ID} where ID is the identity of which the adversary wishes to be challenged. According to the specification of games $\mathbf{G}_2$ and $\mathbf{G}_3$, V and p_{ID} assume the same value in both games. Let us now consider the value $e^* = \log_{g_1} c^*$ which assumes different values in games $\mathbf{G}_2$ and $\mathbf{G}_3$. In particular, while in game $\mathbf{G}_2$, e^* contains information about the message m_σ, in game $\mathbf{G}_3$, it is just a random value. Let us denote with $[e^*]_2$ and $[e^*]_3$ the values of e^* in games $\mathbf{G}_2$ and $\mathbf{G}_3$, respectively.

By definition of game $\mathbf{G}_2$, event T_2 solely depends on $(V, p_{\mathsf{ID}}, [e^*]_2)$. Similarly, by definition of game $\mathbf{G}_3$, event T_3 solely depends on $(V, p_{\mathsf{ID}}, [e^*]_3)$. Moreover, event T_2 depends on $(V, p_{\mathsf{ID}}, [e^*]_2)$ according to the same functional dependence of event T_3 upon $(V, p_{\mathsf{ID}}, [e^*]_3)$. Therefore, to prove the lemma, it suffices to show that $(V, p_{\mathsf{ID}}, [e^*]_2)$ and $(V, p_{\mathsf{ID}}, [e^*]_3)$ have the same distribution.

According to the specification of game $\mathbf{G}_3$, $[e^*]_3$ is chosen uniformly over Z_q, independently from V and p_{ID}. Hence to reach the thesis, it suffices to prove that the distribution of $[e^*]_2$, conditioned on V and p_{ID} is also uniform in Z_q.

In game $\mathbf{G}_2$, the quantities $(V, p_{\mathsf{ID}}, [e^*]_2)$ are related according to the following matrix equation:

$$\begin{pmatrix} p_{\mathsf{ID}} \\ [e^*]_2 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & w \\ r_1^* & wr_2^* \end{pmatrix}}_{M} \cdot \begin{pmatrix} p_{1,\mathsf{ID}} \\ p_{2,\mathsf{ID}} \end{pmatrix} + \begin{pmatrix} 0 \\ \log_{g_1} m_\sigma \end{pmatrix}$$

where $\det(M) = w(r_2^* - r_1^*) \neq 0$, since $r_2^* \neq r_1^*$.

As soon as we fix the value of V, the matrix M is completely fixed, but the values $p_{1,\mathsf{ID}}$ and $p_{2,\mathsf{ID}}$ are still uniformly and independently distributed over Z_q. Now, fixing the value for p_{ID} also fixes a value for m_σ. Hence by Lemma 2, we can conclude that the conditioned distribution of $[e^*]_2$, w.r.t. V and p_{ID}, is also uniform over Z_q. □

Proofs of the Lemmas stated in Theorem 3

Lemma 4. $\Pr[T_4] = \Pr[T_3]$ *and* $\Pr[R_4] = \Pr[R_3]$.

Proof. Consider the quantities

$$V := (Coins, H, w, f_{1,\mathsf{ID}}, f_{2,\mathsf{ID}}, h_{1,\mathsf{ID}}, h_{2,\mathsf{ID}}, \sigma, r_1^*, r_2^*)$$

and the value p_{ID} where ID is the identity of which the adversary wishes to be challenged. Applying the same notations and reasons as in Lemma 3, we can notice that event T_3 solely depends on $(V, p_{\mathsf{ID}}, [e^*]_3)$. Similarly, event T_4 solely depends on $(V, p_{\mathsf{ID}}, [e^*]_4)$. The same considerations hold for events R_3 and R_4. Therefore, to prove the lemma, it suffices to show that $(V, p_{\mathsf{ID}}, [e^*]_3)$ and $(V, p_{\mathsf{ID}}, [e^*]_4)$ have the same distribution.

According to the specification of game $\mathbf{G}_4$, $[e^*]_4$ is chosen uniformly over Z_q, independently from V and p_{ID}. Hence to reach the thesis, it suffices to prove that the distribution of $[e^*]_3$, conditioned on V and p_{ID}, is also uniform in Z_q.

In game $\mathbf{G}_3$, the quantities $(V, p_{\mathsf{ID}}, [e^*]_3)$ are related according to the following matrix equation:

$$\begin{pmatrix} p_{\mathsf{ID}} \\ [e^*]_3 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & w \\ r_1^* & wr_2^* \end{pmatrix}}_{M} \cdot \begin{pmatrix} p_{1,\mathsf{ID}} \\ p_{2,\mathsf{ID}} \end{pmatrix} + \begin{pmatrix} 0 \\ \log_{g_1} m_\sigma \end{pmatrix}$$

where $\det(M) = w(r_2^* - r_1^*) \neq 0$, since $r_2^* \neq r_1^*$.

As soon as we fix the value of V, the matrix M is completely fixed, but the values $p_{1,\mathsf{ID}}$ and $p_{2,\mathsf{ID}}$ are still uniformly and independently distributed over Z_q. Now, fixing a value for p_{ID} also fixes a value for m_σ. Hence by Lemma 2, we can conclude that the conditioned distribution of $[e^*]_3$, w.r.t. V and p_{ID}, is also uniform over Z_q. □

Lemma 5. $\Pr[R_5] \leq \frac{Q_A(\lambda)}{q}$, *where* $Q_A(\lambda)$ *is an upper bound on the number of decryption queries* A *made.*

Proof. For $1 \leq i \leq Q_A(\lambda)$, we define $R_5^{(i)}$ to be the event that the i-th ciphertext $\langle \mathsf{ID}_i, C_i \rangle$, submitted by A to the decryption oracle in game $\mathbf{G}_5$, fails the test in step $D2'$, but would have passed the test in step $D2$ in game $\mathbf{G}_2$. Furthermore, for $1 \leq i \leq Q_A(\lambda)$, we define $B_5^{(i)}$ and $\hat{B}_5^{(i)}$ respectively to be the events that the i-th ciphertext is submitted to the decryption oracle before and after A received its challenge. The bound is proven if we can show that, for $1 \leq i \leq Q_A(\lambda)$, $\Pr[R_5^{(i)} | B_5^{(i)}] \leq \frac{1}{q}$ and that $\Pr[R_5^{(i)} | \hat{B}_5^{(i)}] \leq \frac{1}{q}$.

Claim 1: $\Pr[R_5^{(i)} | B_5^{(i)}] \leq \frac{1}{q}$.
To proof this claim, fix $1 \leq i \leq Q_A(\lambda)$.

Consider the quantities:

$$V := (Coins, H, w, p_{\mathsf{ID}_i}), \quad V' := (f_{\mathsf{ID}_i}, h_{\mathsf{ID}_i}).$$

The values of V and V' completely determine the behaviour of A up to the moment A performs the encryption query. In particular, they completely determine the event $B_5^{(i)}$. We say V and V' are relevant if the event $B_5^{(i)}$ occurs.

Hence it will suffice to prove that the probability that event $R_5^{(i)}$ occurs conditioned on any fixed relevant values of V and V', is bounded by $1/q$.

Recall that the condition tested in step $D2'$ in game $\mathbf{G}_5$ is $u_2 = u_1^w$ and $v = u_1^{(f_{1,\mathsf{ID}_i}+h_{1,\mathsf{ID}_i}\alpha)+(f_{2,\mathsf{ID}_i}+h_{2,\mathsf{ID}_i}\alpha)w}$. Since we are considering the case that the i-query fails the step in $D2'$ but would have passed the test in step $D2$ of game $\mathbf{G}_2$, it must be the case that $u_2 \neq u_1^w$ and $v = u_1^{(f_{1,\mathsf{ID}_i}+h_{1,\mathsf{ID}_i}\alpha)} \cdot u_2^{(f_{2,\mathsf{ID}_i}+h_{2,\mathsf{ID}_i}\alpha)w}$. Therefore, we only need to consider values of V and V' such that $u_2 \neq u_1^w$. Taking the logs (base g_1), the condition $u_2 \neq u_1^w$ is equivalent to $r_1 \neq r_2$ and the condition $v = u_1^{(f_{1,\mathsf{ID}_i}+h_{1,\mathsf{ID}_i}\alpha)} \cdot u_2^{(f_{2,\mathsf{ID}_i}+h_{2,\mathsf{ID}_i}\alpha)w}$ is equivalent to the condition $x_{\mathsf{ID}_i} = y_{\mathsf{ID}_i}$, where $x_{\mathsf{ID}_i} := \log_{g_1} v$ and $y_{\mathsf{ID}_i} := r_1 f_{1,\mathsf{ID}_i} + r_2 w f_{2,\mathsf{ID}_i} + r_1 h_{1,\mathsf{ID}_i}\alpha + r_2 w h_{2,\mathsf{ID}_i}\alpha$.

Thus we have

$$\begin{pmatrix} f_{\mathsf{ID}_i} \\ h_{\mathsf{ID}_i} \\ y_{\mathsf{ID}_i} \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & w & 0 & 0 \\ 0 & 0 & 1 & w \\ r_1 & r_2 w & r_1\alpha & r_2\alpha w \end{pmatrix}}_{M} \cdot \begin{pmatrix} f_{1,\mathsf{ID}_i} \\ f_{2,\mathsf{ID}_i} \\ h_{1,\mathsf{ID}_i} \\ h_{2,\mathsf{ID}_i} \end{pmatrix}$$

Clearly, the first two rows of matrix M are linearly independent. It is easy to see that the third row is independent from the others, notice that the only way to obtain r_1 is by multiplying the first row by r_1, doing so, the second component of the first row results to be $r_1 w$. However, the second component of the third row has value $r_2 w$, this contradicts the condition $r_1 \neq r_2$.

As soon as we fix V, the first two rows of matrix M are fixed, but the values $f_{1,\mathsf{ID}_i}, f_{2,\mathsf{ID}_i}, h_{1,\mathsf{ID}_i}, h_{2,\mathsf{ID}_i}$ are still uniformly and independently distributed over Z_q. Let us further condition on a fixed value of V' such that V and V' are relevant and that $r_1 \neq r_2$. This fixes the third row of M along with the values $f_{\mathsf{ID}_i}, h_{\mathsf{ID}_i}$ and x_{ID_i}. It follows from Lemma 2 that y_{ID_i} is still uniformly distributed over Z_q, but since x_{ID_i} is fixed, we have $\Pr[x_{\mathsf{ID}_i} = y_{\mathsf{ID}_i}] = 1/q$.

Claim 2: $\Pr[R_5^{(i)} | \hat{B}_5^{(i)}] \leq \frac{1}{q}$.
To proof this claim, fix $1 \leq i \leq Q_A(\lambda)$.
First, we consider the case when $\mathsf{ID}_i = \mathsf{ID}$.

Consider the quantities

$$V := (Coins, H, w, p_{\mathsf{ID}}, r_1^*, r_2^*, e^*), V' := (f_{\mathsf{ID}}, h_{\mathsf{ID}}, x_{\mathsf{ID}}^*).$$

The values of V and V' completely determine the entire behaviour of A in game $\mathbf{G}_5$. In particular, they completely determine the event $\hat{B}_5^{(i)}$. We say V and V' are relevant if the event $\hat{B}_5^{(i)}$ occurs.

Hence it will suffice to prove that the probability that event $R_5^{(i)}$ occurs, conditioned on any fixed relevant values of V and V', is bounded by $1/q$.

As shown earlier, we consider only relevant values of V and V' for which $r_1 \neq r_2$. Reasoning as above, and using the same notations, we have the following matrix equation,

$$\begin{pmatrix} f_{\mathsf{ID}} \\ h_{\mathsf{ID}} \\ x^*_{\mathsf{ID}} \\ y_{\mathsf{ID}} \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & w & 0 & 0 \\ 0 & 0 & 1 & w \\ r_1^* & r_2^* w & r_1^* \alpha^* & r_2^* \alpha^* w \\ r_1 & r_2 w & r_1 \alpha & r_2 \alpha w \end{pmatrix}}_{M} \cdot \begin{pmatrix} f_{1,\mathsf{ID}} \\ f_{2,\mathsf{ID}} \\ h_{1,\mathsf{ID}} \\ h_{2,\mathsf{ID}} \end{pmatrix}$$

where M is a 4 by 4 matrix. Notice that the assumption that the i-query $\langle \mathsf{ID}_i, C_i \rangle$ where $C_i = \langle u_1, u_2, c \rangle$ is rejected in step $D2'$ implies that C_i passed the *special rejection rule*. Furthermore, we may assume that $\alpha \neq \alpha^*$, since otherwise the only way C_i may have passed the *special rejection rule* is that $\langle u_1, u_2, c \rangle = \langle u_1^*, u_2^*, c^* \rangle$.

Hence it is easy to see that the rows of M are linearly independent, since

$$\det(M) = w^2(r_2 - r_1)(r_2^* - r_1^*)(\alpha^* - \alpha) \neq 0.$$

As soon as we fix V, the first three rows of matrix M are fixed, but the values $f_{1,\mathsf{ID}}, f_{2,\mathsf{ID}}, h_{1,\mathsf{ID}}, h_{2,\mathsf{ID}}$ are still uniformly and independently distributed over Z_q. Let us further condition on a fixed value of V' such that V and V' are relevant and that $r_1 \neq r_2$ and $\alpha \neq \alpha^*$. This fixes the fourth row of M along with the values $f_{\mathsf{ID}}, h_{\mathsf{ID}}, x^*_{\mathsf{ID}}$ and x_{ID}. It follows from Lemma 2 that y_{ID} is still uniformly distributed over Z_q, but since x_{ID} is fixed, we have $\Pr[x_{\mathsf{ID}} = y_{\mathsf{ID}}] = 1/q$.

Second, we consider the case when $\mathsf{ID}_i \neq \mathsf{ID}$.

Consider the quantities

$$V := (Coins, H, w, p_{\mathsf{ID}}, p_{\mathsf{ID_i}}, r_1^*, r_2^*, e^*), V' := (f_{\mathsf{ID}}, h_{\mathsf{ID}}, f_{\mathsf{ID}_i}, h_{\mathsf{ID}_i}, x^*_{\mathsf{ID}}).$$

The values of V and V' completely determine the entire behaviour of A in game $\mathbf{G}_5$. In particular, they completely determine the event $\hat{B}_5^{(i)}$. We say V and V' are relevant if the event $\hat{B}_5^{(i)}$ occurs.

Hence it will suffice to prove that the probability that event $R_5^{(i)}$ occurs conditioned on any fixed relevant values of V and V', is bounded by $1/q$.

As shown earlier, we consider only relevant values of V and V' for which $r_1 \neq r_2$. Thus we have the following matrix equation,

$$\begin{pmatrix} f_{\mathsf{ID}} \\ h_{\mathsf{ID}} \\ f_{\mathsf{ID}_i} \\ h_{\mathsf{ID}_i} \\ x^*_{\mathsf{ID}} \\ y_{\mathsf{ID}_i} \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & w & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & w & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & w & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & w \\ r_1^* & r_2^* w & r_1^* \alpha^* & r_2^* \alpha^* w & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & r_1 & r_2 w & r_1 \alpha & r_2 \alpha w \end{pmatrix}}_{M} \cdot \begin{pmatrix} f_{1,\mathsf{ID}} \\ f_{2,\mathsf{ID}} \\ h_{1,\mathsf{ID}} \\ h_{2,\mathsf{ID}} \\ f_{1,\mathsf{ID}_i} \\ f_{2,\mathsf{ID}_i} \\ h_{1,\mathsf{ID}_i} \\ h_{2,\mathsf{ID}_i} \end{pmatrix}$$

Clearly, the first four rows of matrix M are linearly independent. In order to show that the fifth row is independent from the others, notice that the only way to obtain r_1^* is by multiplying the first row by r_1^*, doing so, the second component of the third row results to be $r_1^* w$. However, the second component of the fifth row has value $r_2^* w$, this contradicts the condition $r_1^* \neq r_2^*$. In order to show that the last row is linearly independent from the first five rows, observe that the only way to obtain r_1 is by multiplying the third row by r_1, doing so, the second component of the third row results to be $r_1 w$. However, the second component of the fifth row has value $r_2 w$, this contradicts the condition $r_1 \neq r_2$.

As soon as we fix V, the first five rows of matrix M are fixed, but the values $f_{1,\mathsf{ID}}, f_{2,\mathsf{ID}}, h_{1,\mathsf{ID}}, h_{2,\mathsf{ID}}, f_{1,\mathsf{ID}_i}, f_{2,\mathsf{ID}_i}, h_{1,\mathsf{ID}_i}, h_{2,\mathsf{ID}_i}$ are still uniformly and independently distributed over Z_q. Let us further condition on a fixed value of V' such that V and V' are relevant and that $r_1 \neq r_2$ and $\alpha \neq \alpha^*$. This fixes the sixth row of M along with the values $f_{\mathsf{ID}}, h_{\mathsf{ID}}, f_{\mathsf{ID}_i}, h_{\mathsf{ID}_i}, x_{\mathsf{ID}}^*$ and x_{ID_i}. It follows from Lemma 2 that y_{ID_i} is still uniformly distributed over Z_q, but since x_{ID_i} is fixed, we have $\Pr[x_{\mathsf{ID}_i} = y_{\mathsf{ID}_i}] = 1/q$. □